

Fig. 1

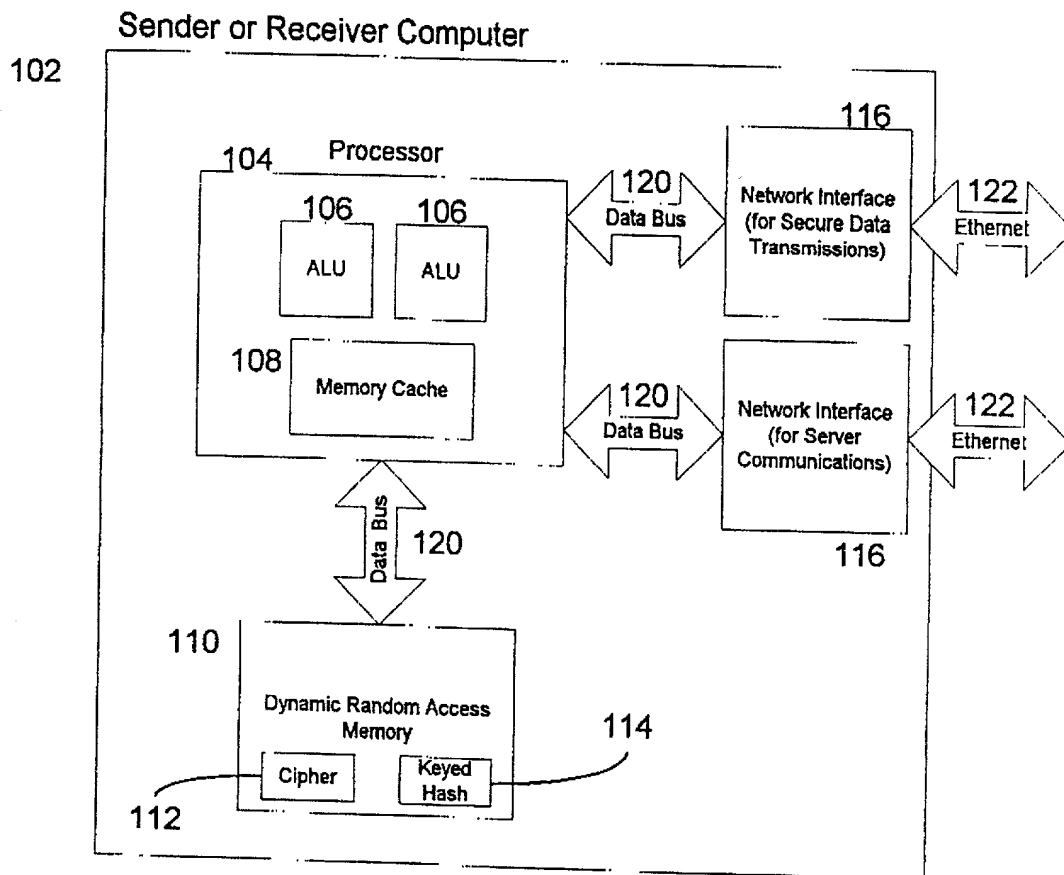
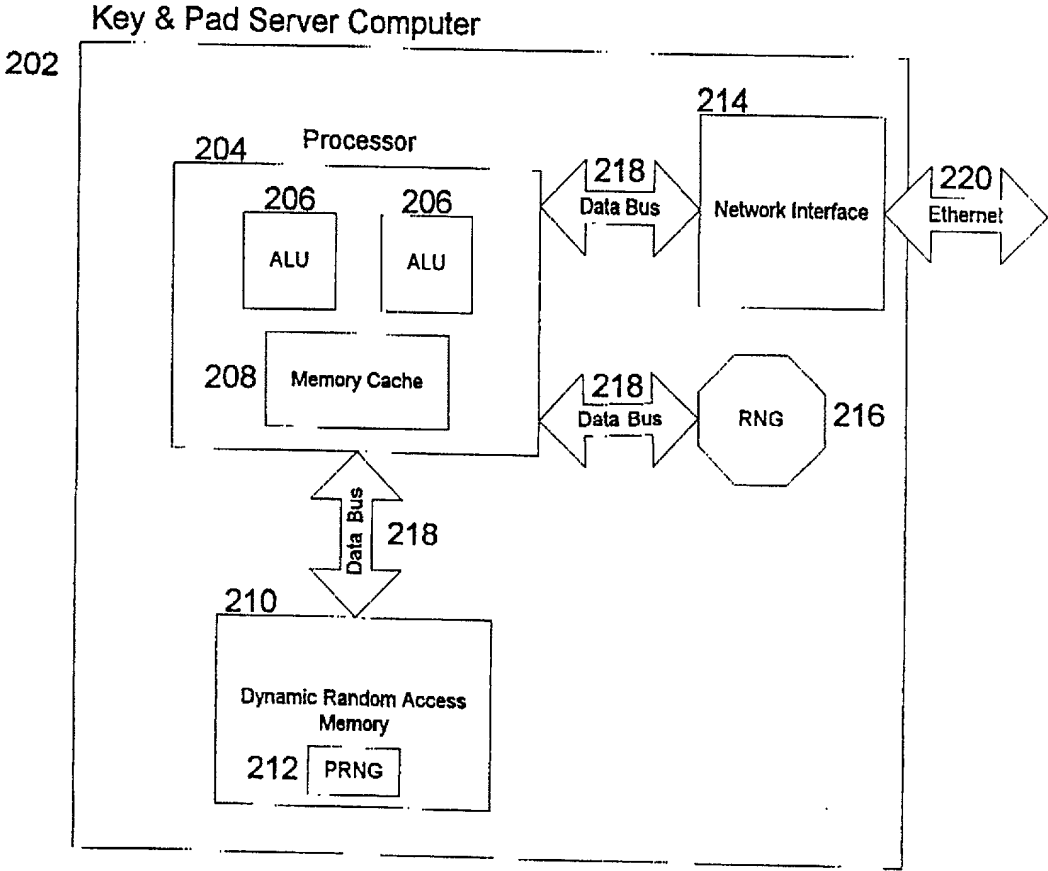


Fig. 2



Simple Mechanism of Generating a Random Permutation of a Sequence of Unique Numbers from 0 to N

Fig. 3

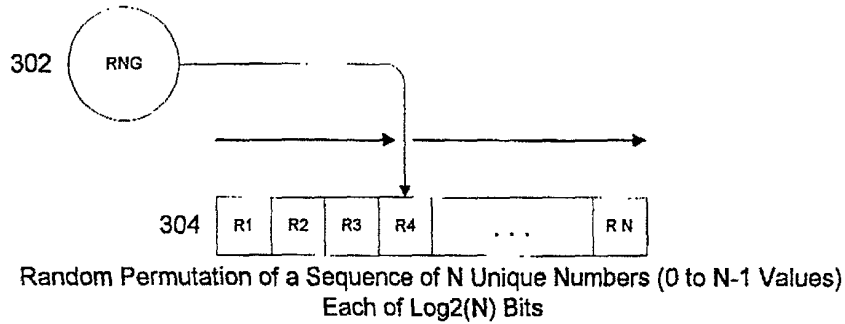


Fig. 4 Near Perfect Riffle Shuffle Mechanism of Generating a Random Permutation of a Sequence of Unique Numbers from 0 to N.

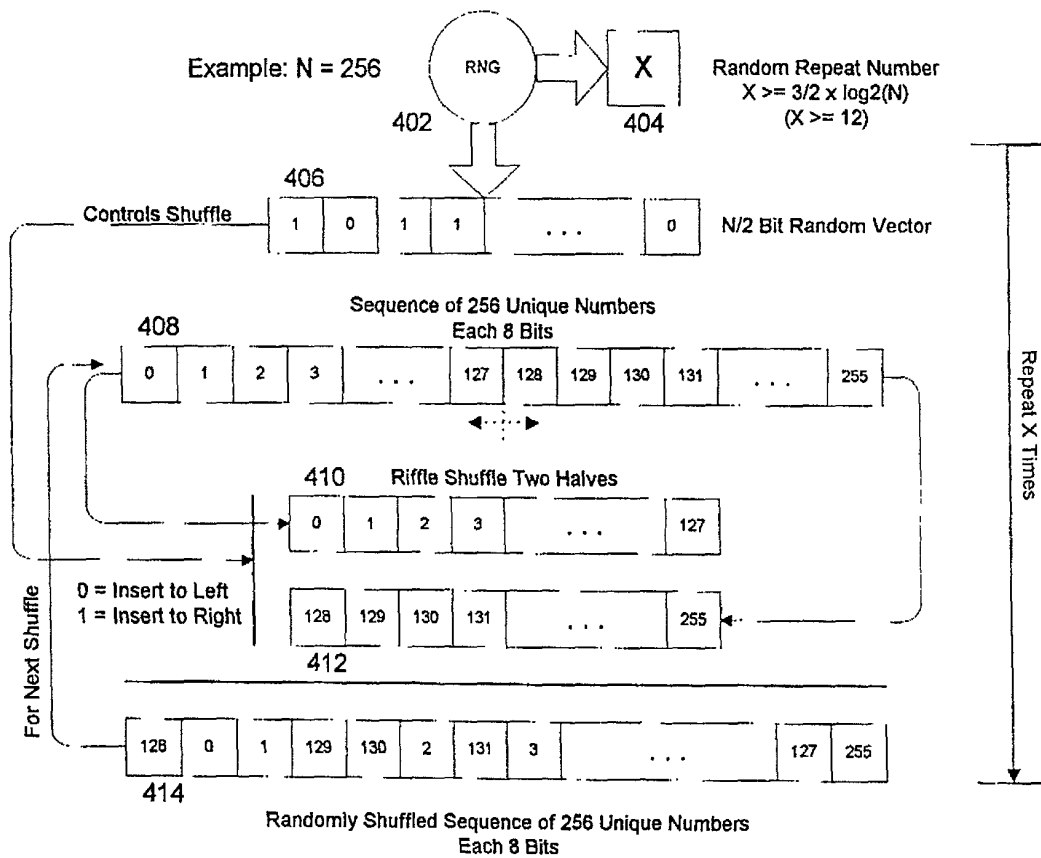


Fig. 5 Randomly Permutating a Sequence of Numbers

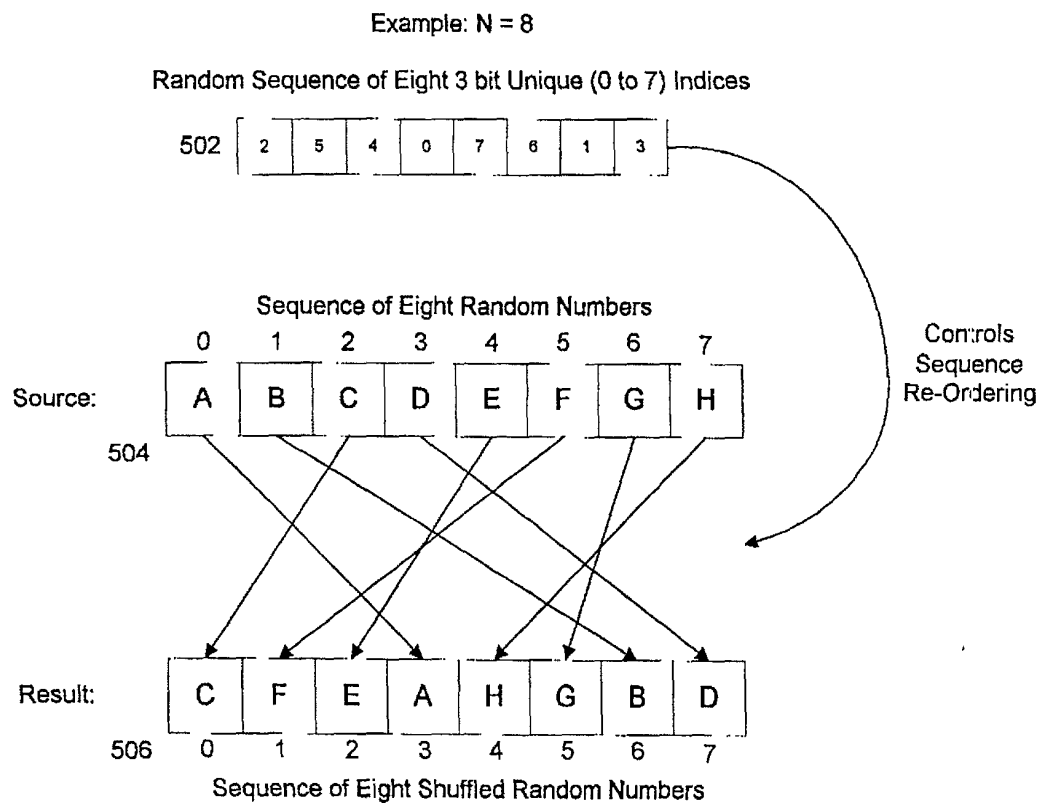


Fig. 6 Key or Seed Data Structure

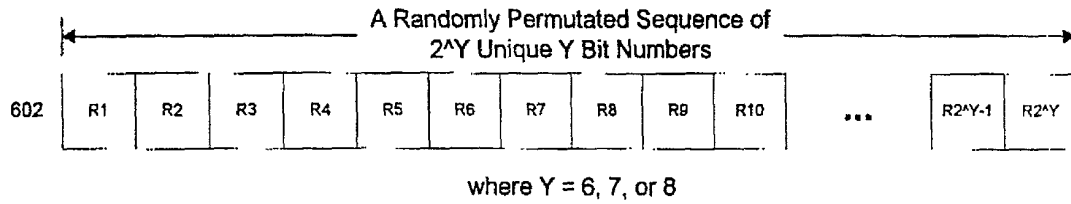


Fig. 7 Unit Sizes Used For Partitioning Random Permutations

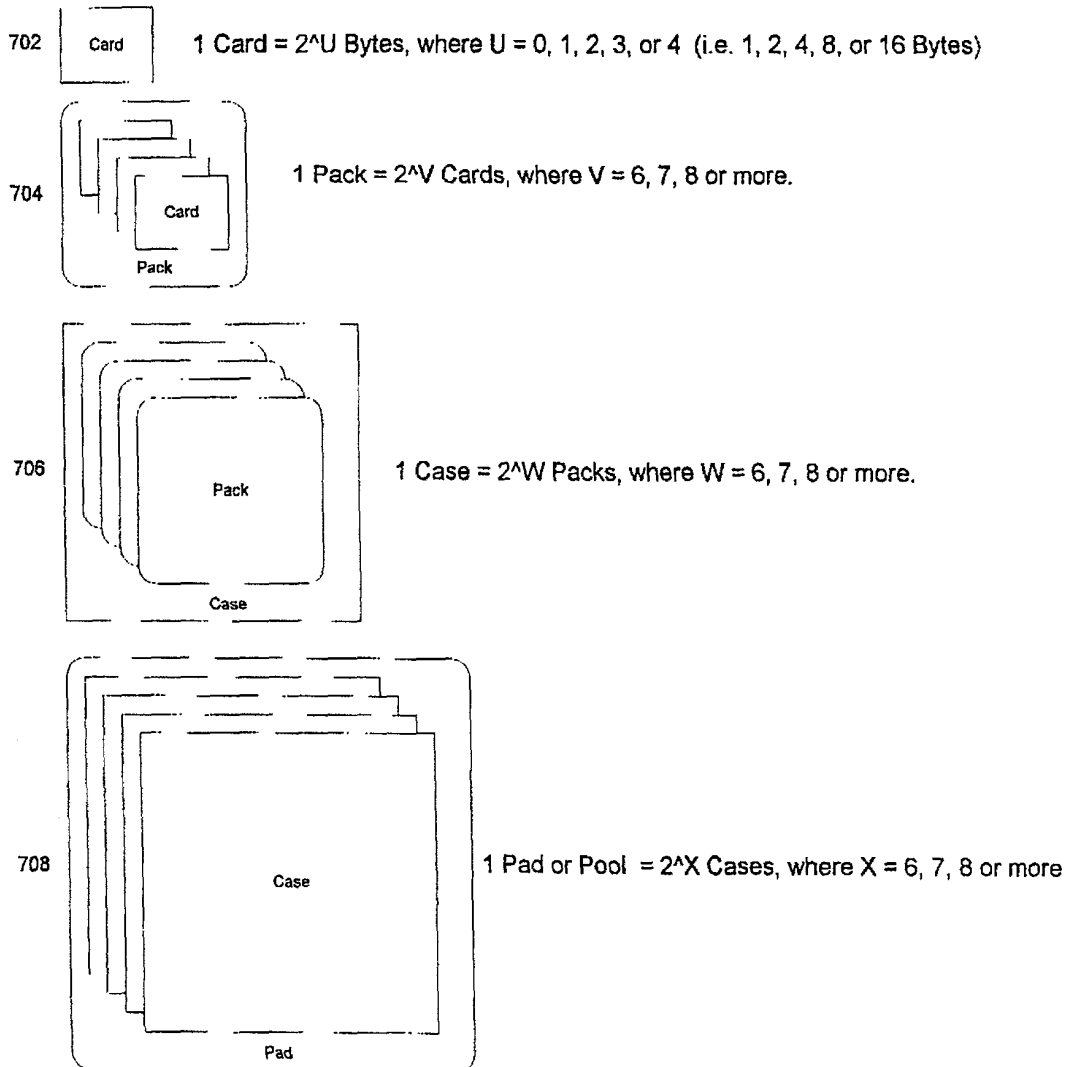


Fig. 8

Flow Chart for Nested Shuffle

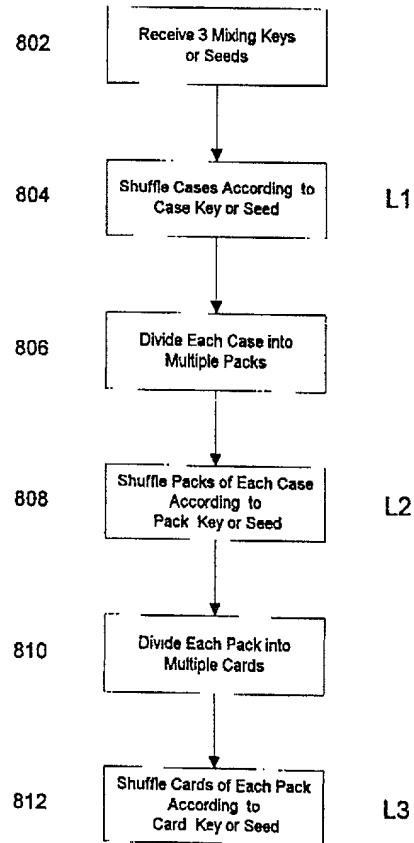


Fig. 9

Nested Shuffle of a Series of Cards

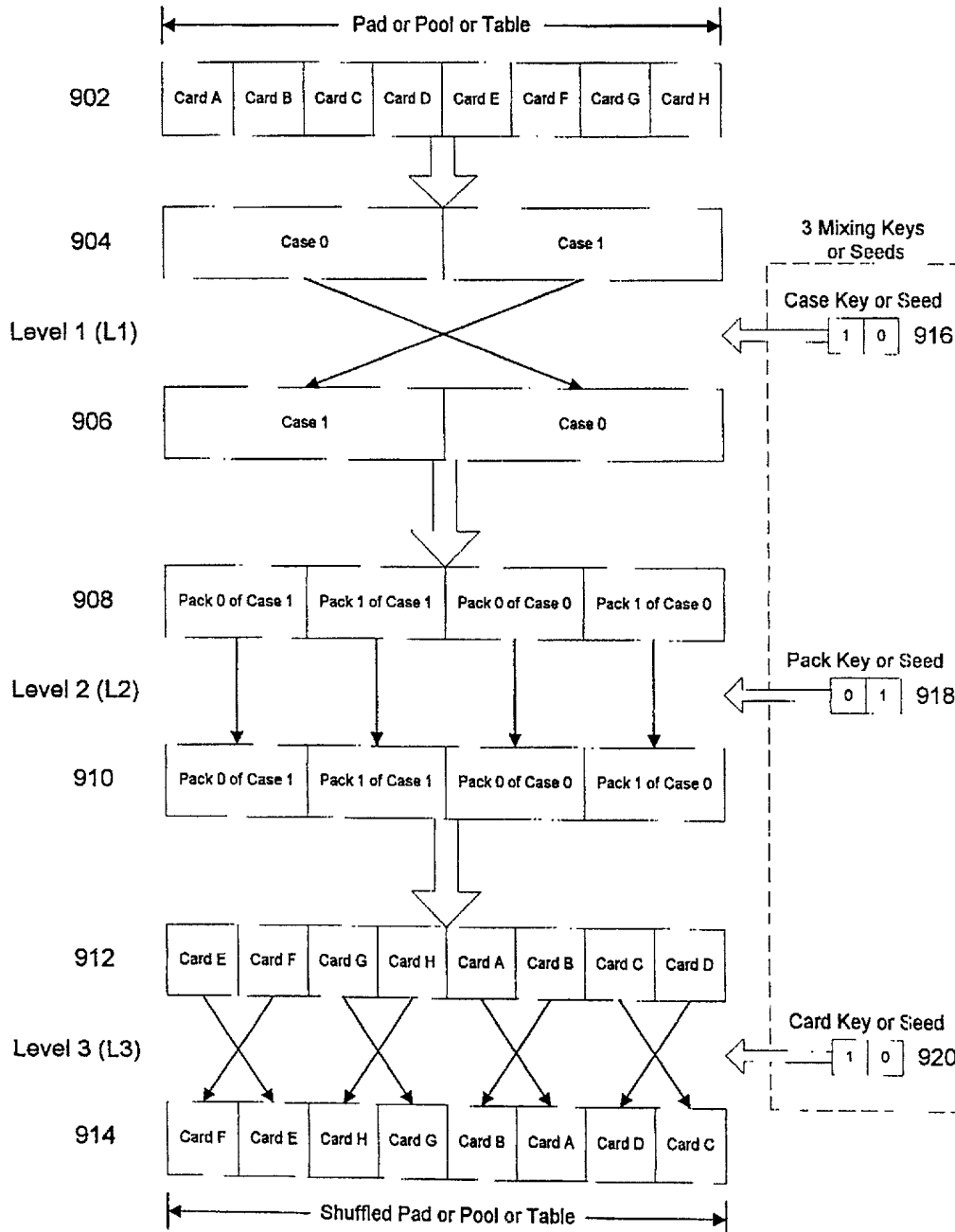


Fig. 10 Non-Cyclic Pseudo-Random Number Generator

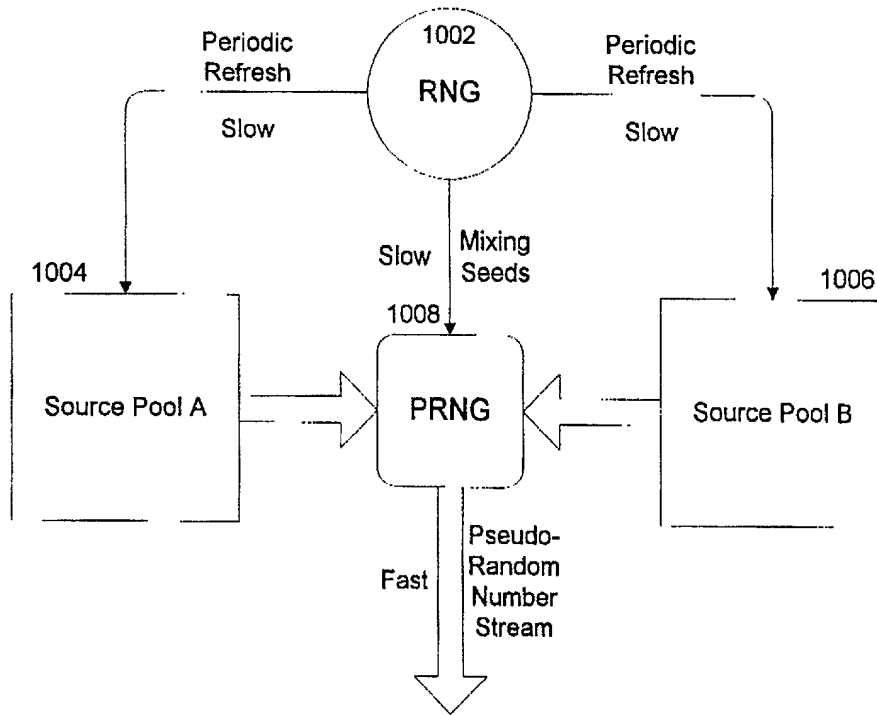


Fig. 11 Non-Cyclic Pseudo-Random Number Generation

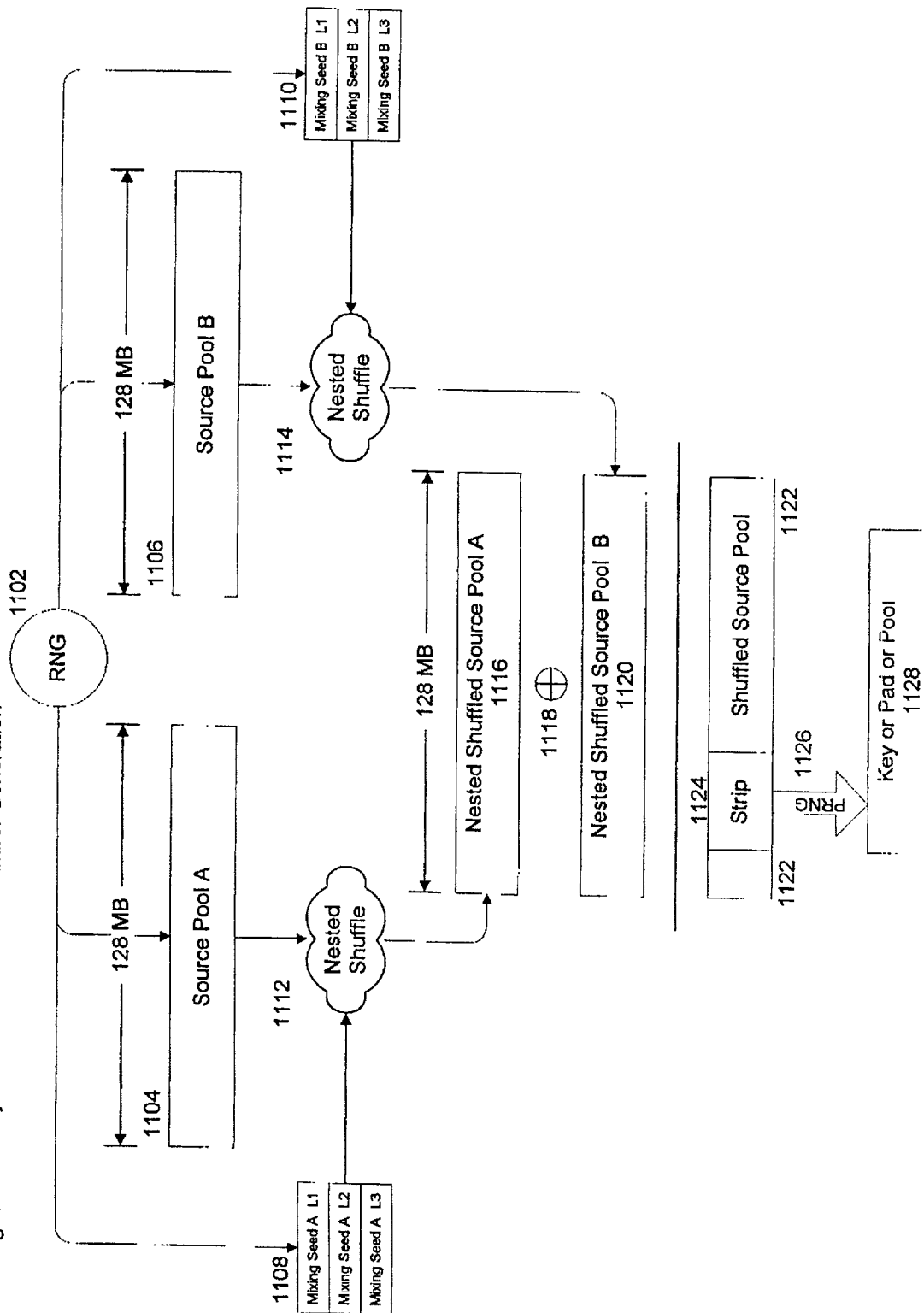


Fig. 12

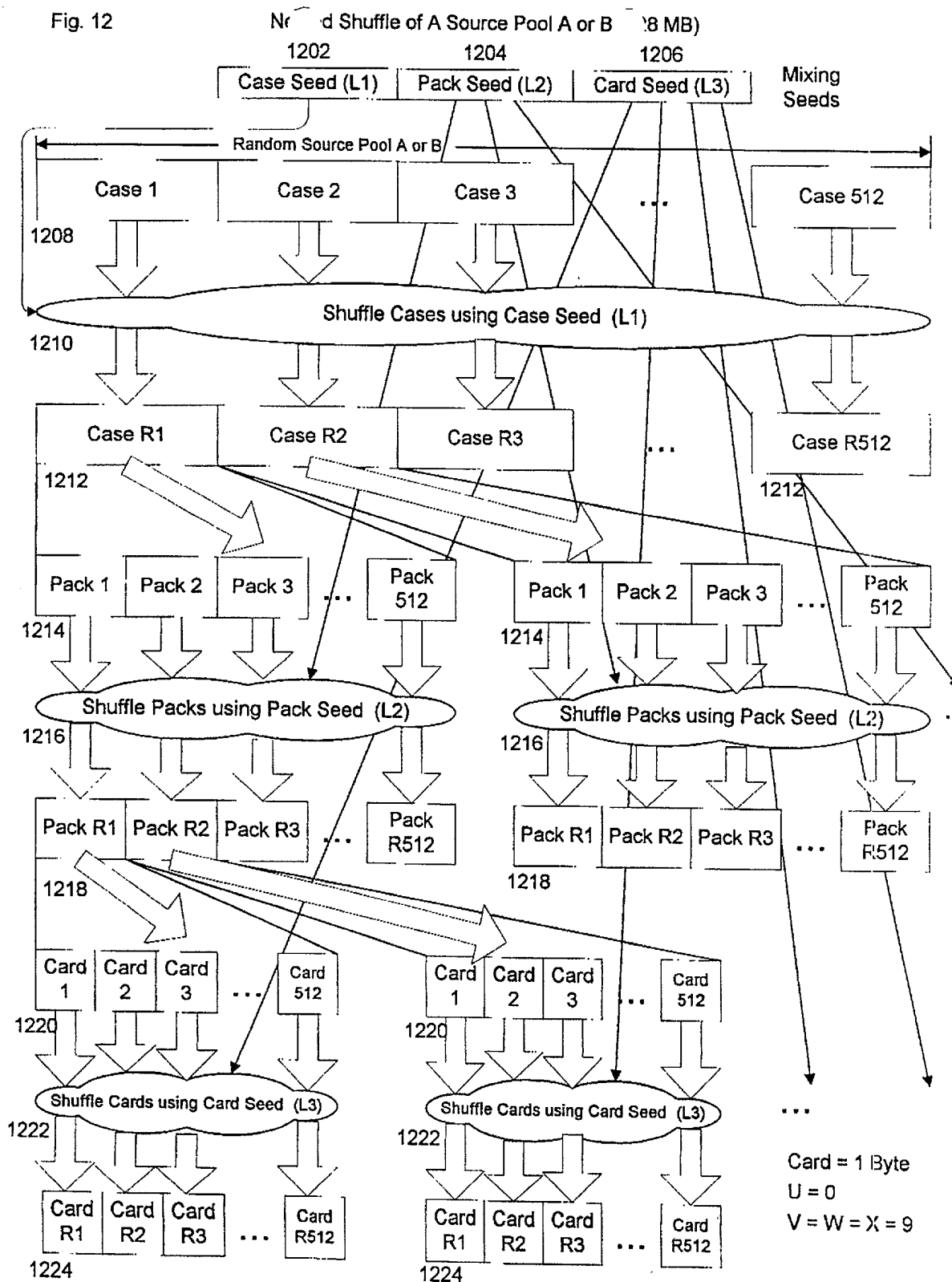
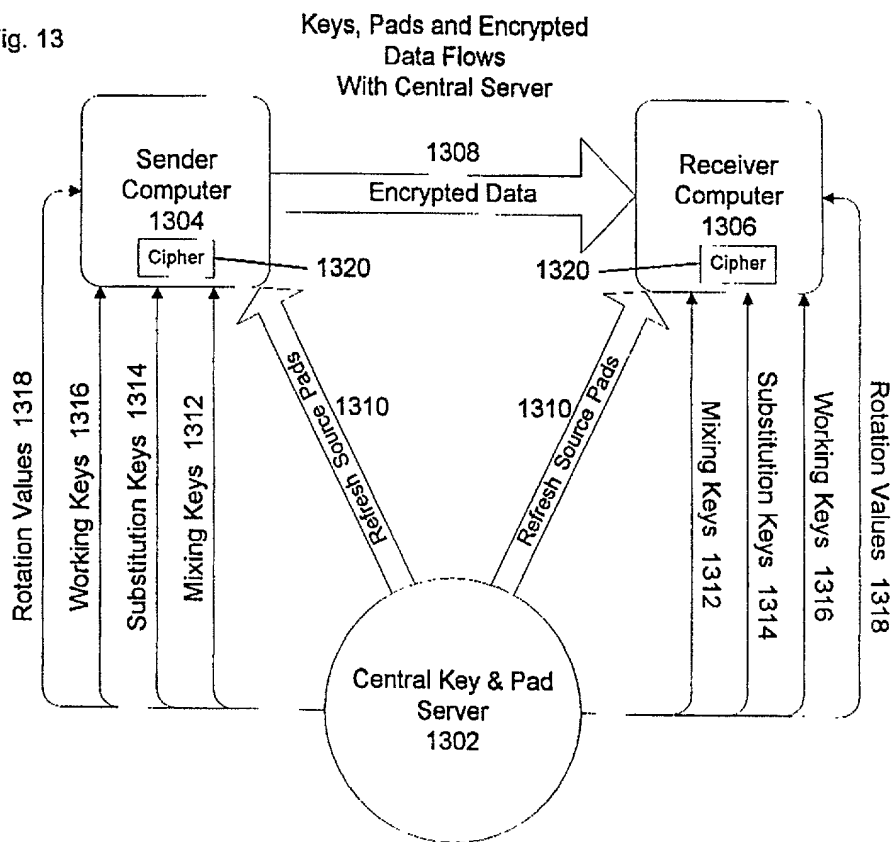


Fig. 13



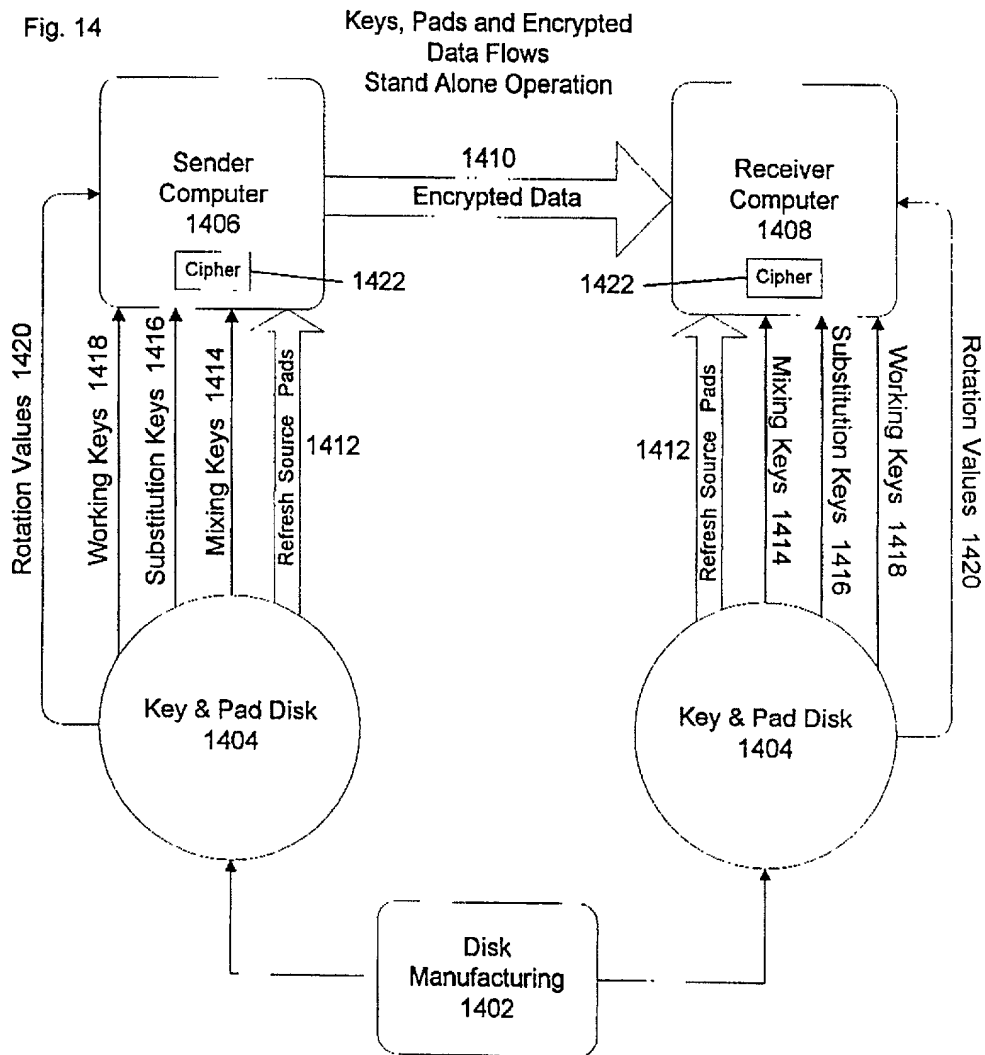


Fig. 15

ENCRYPTION

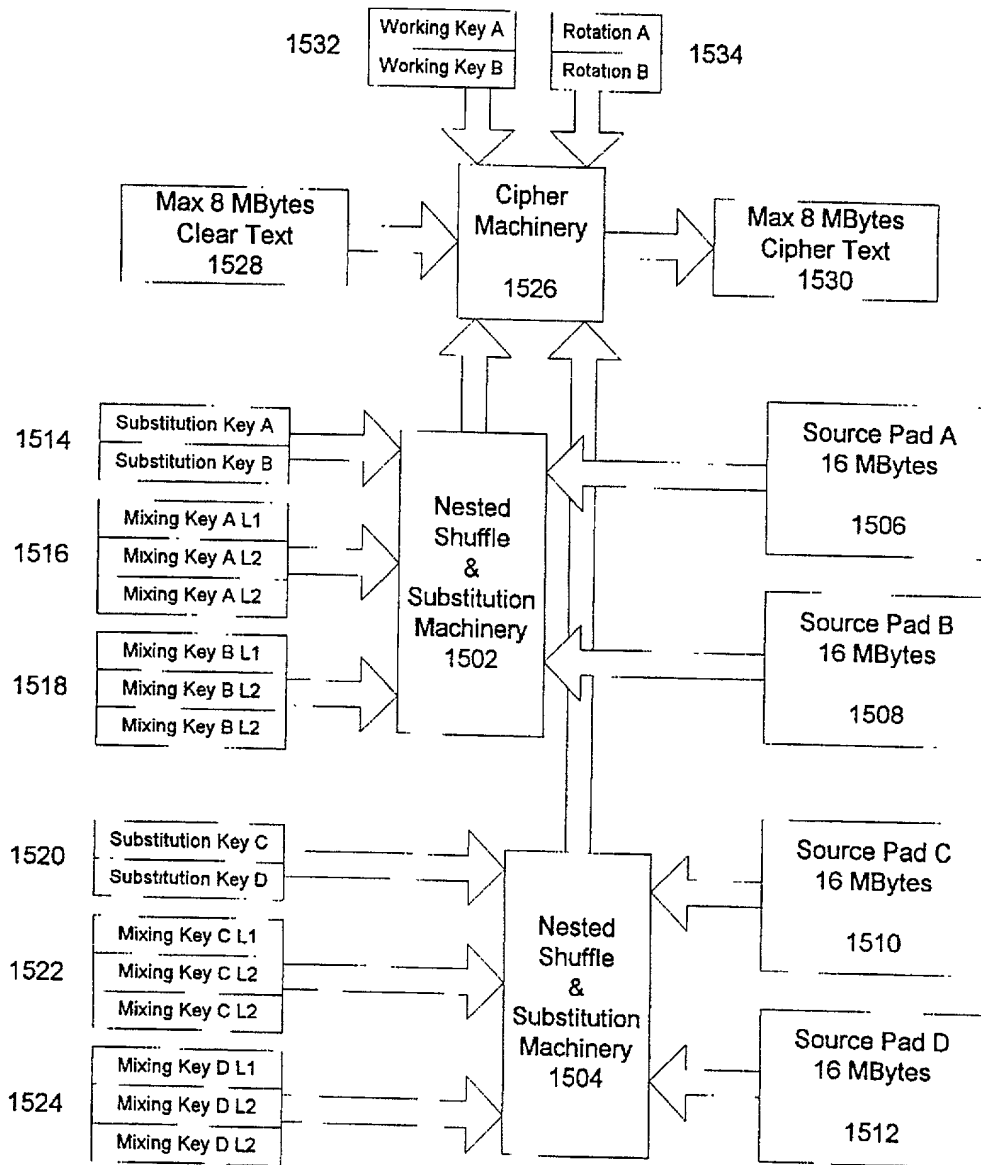


Fig. 16

DECRYPTION

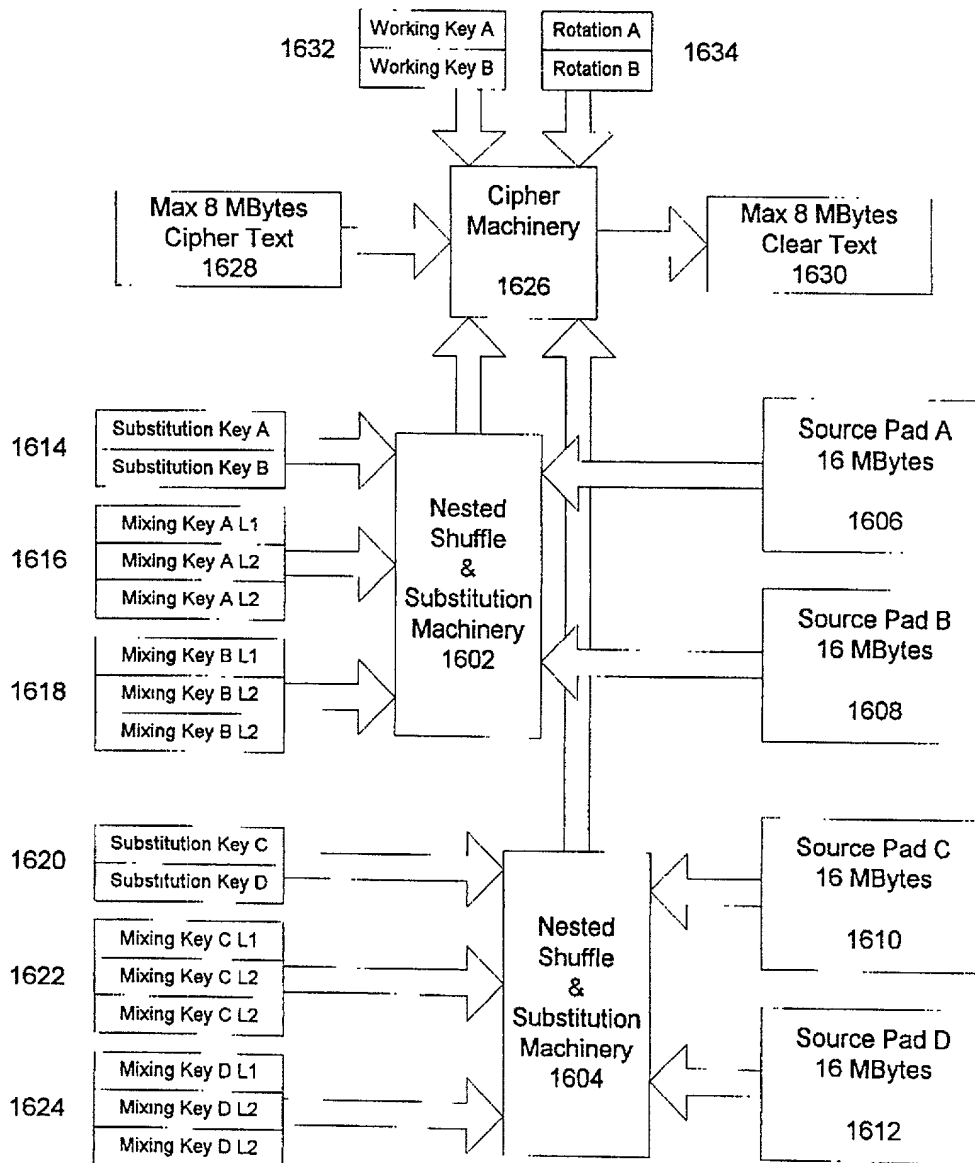


Fig. 17

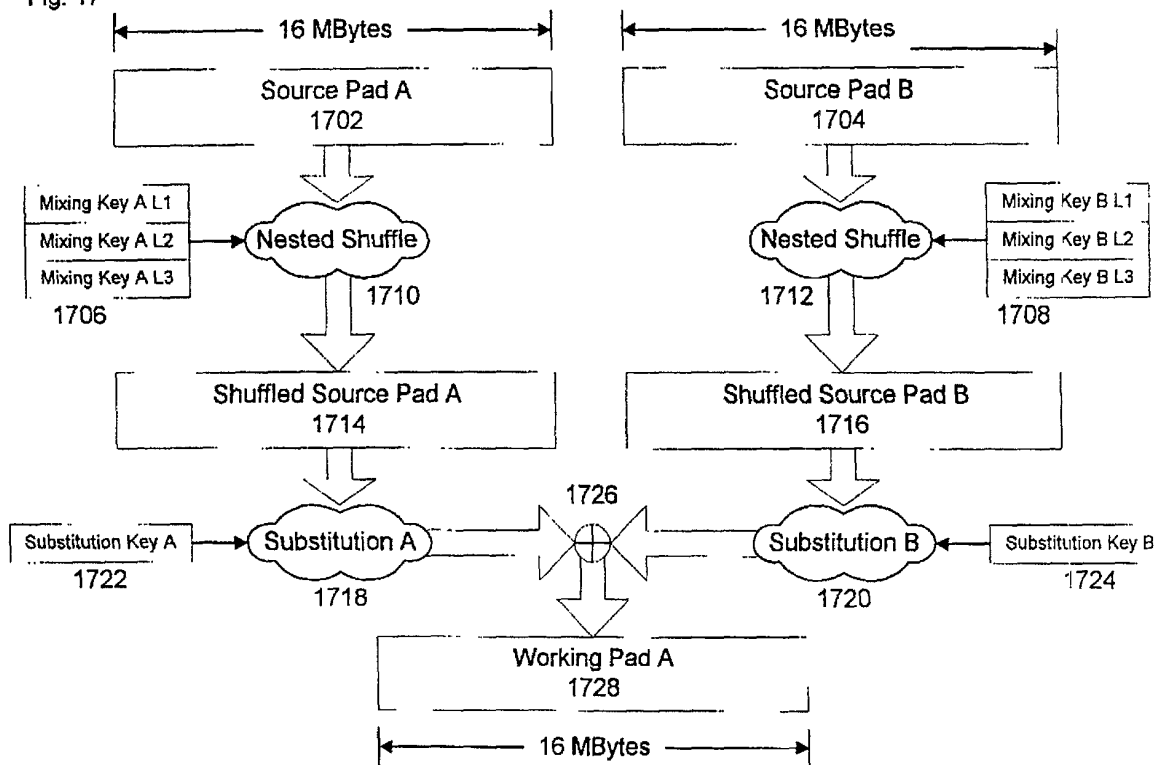


Fig. 18

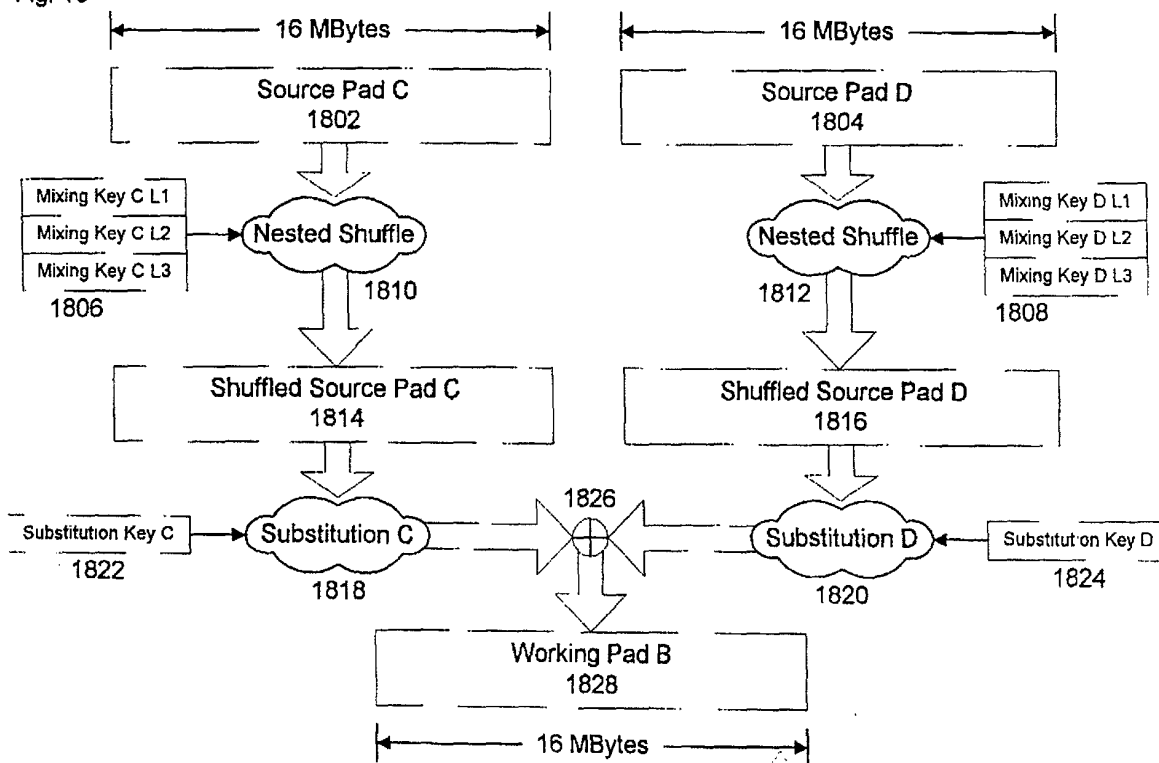


Fig. 19

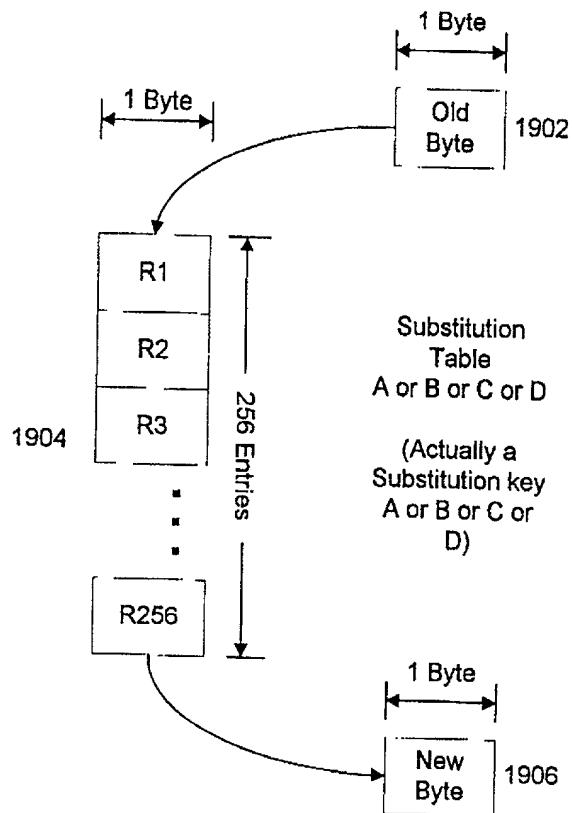


Fig. 20

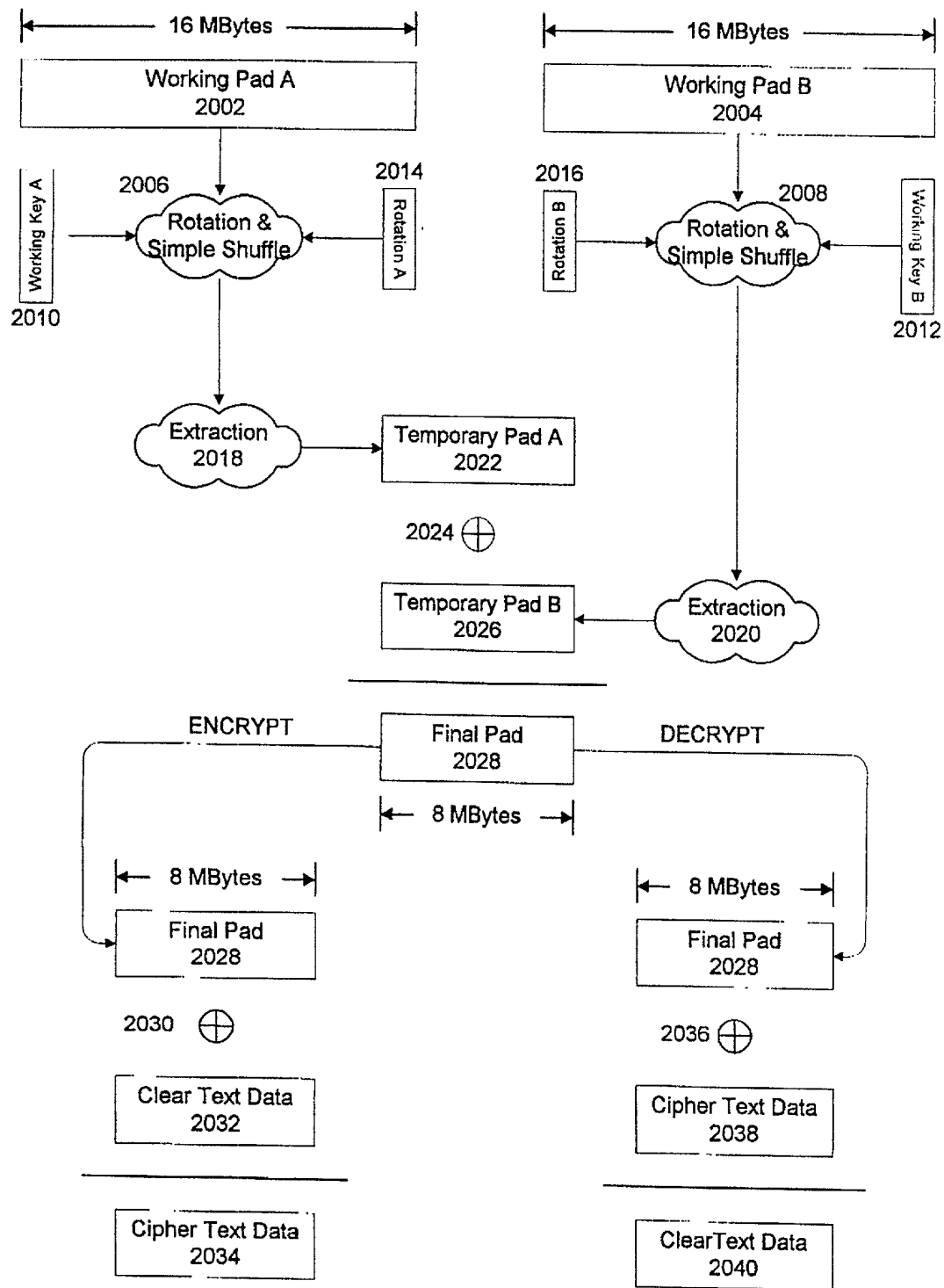


Fig. 21

Shuffled Shuffle Of A Source Pad (16 * 1)

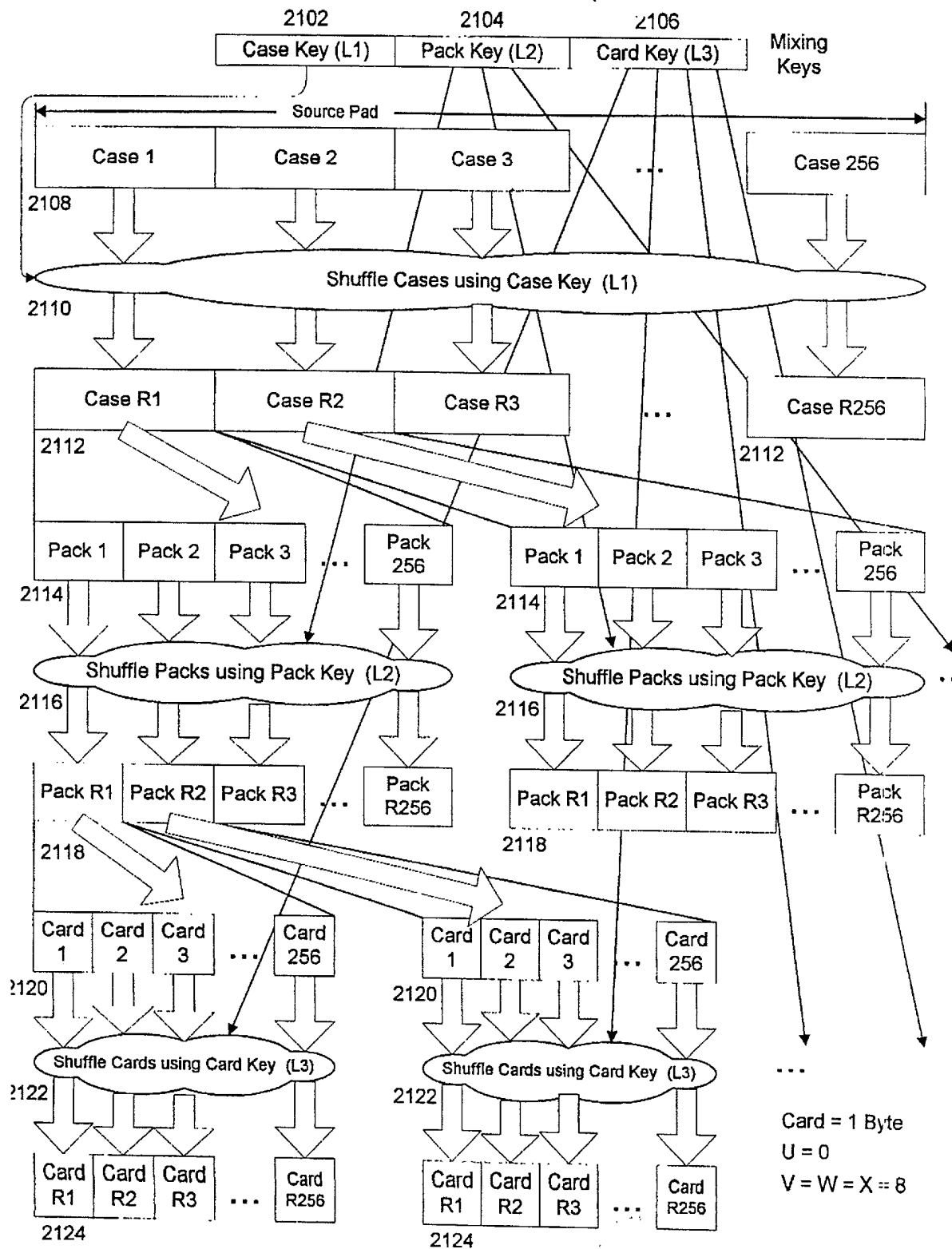


Fig. 22
Rotation & Simple Shuffle of Working Pad (16 MB)
and Extraction of a Temporary Pad (8MB)
Using a Working Key and Rotation Value

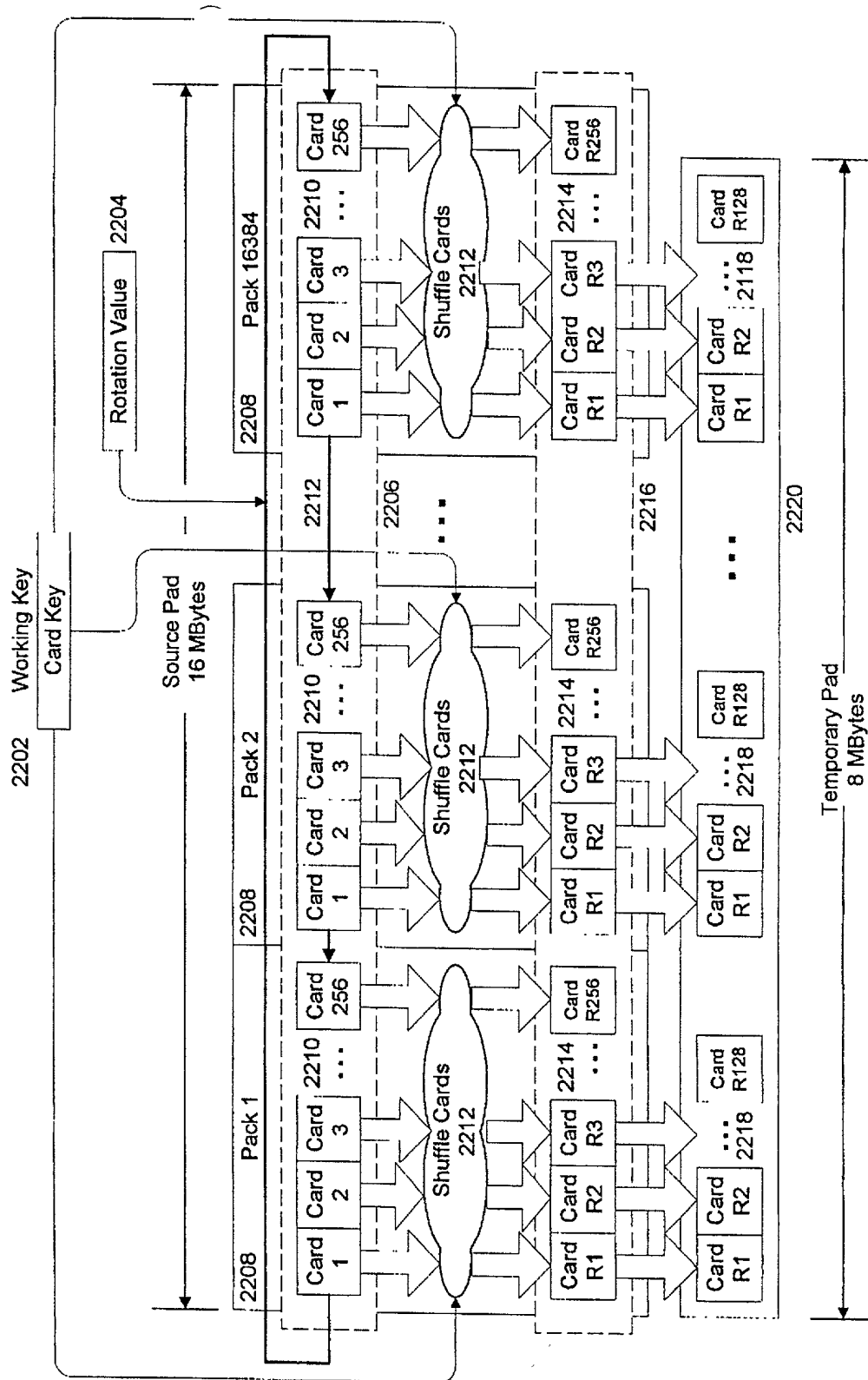


Fig. 23 Keyed One-Way Hash Function

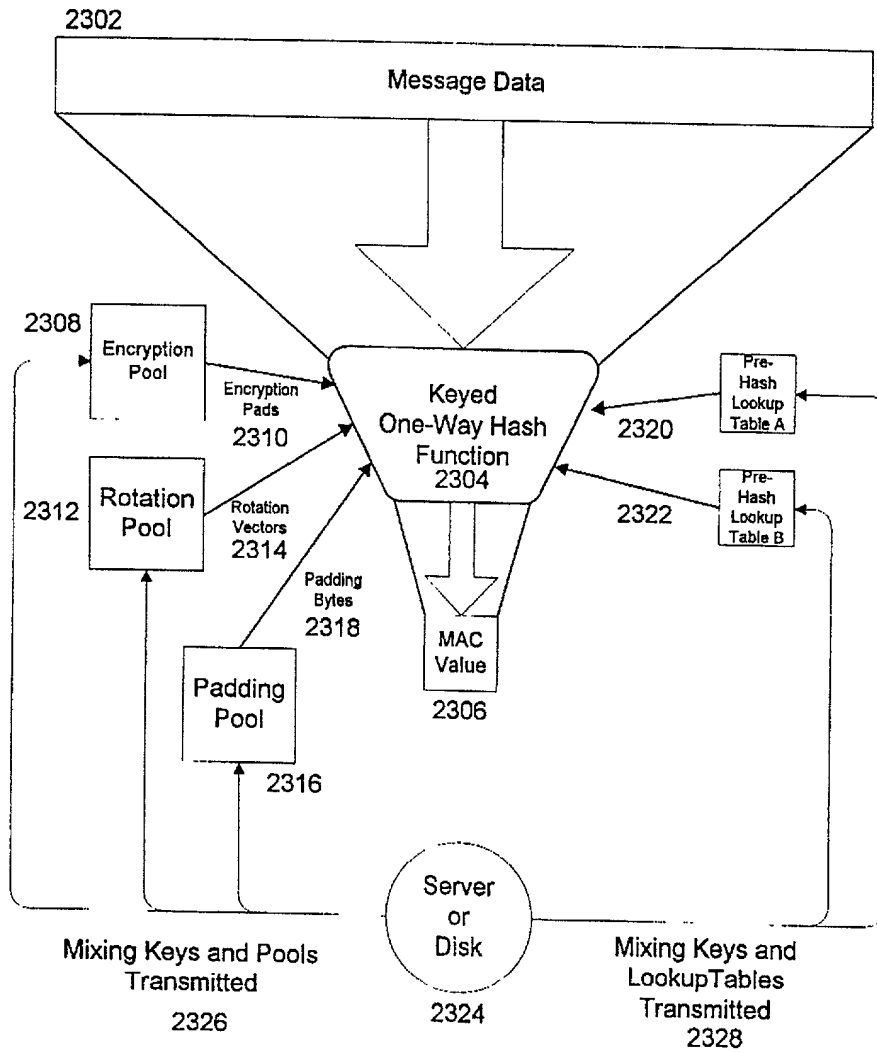


Fig. 24

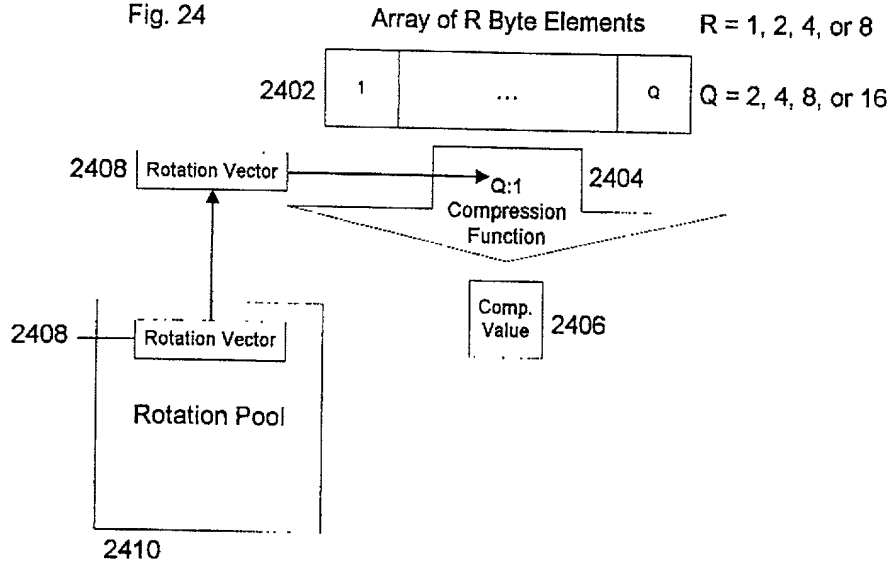


Fig. 25

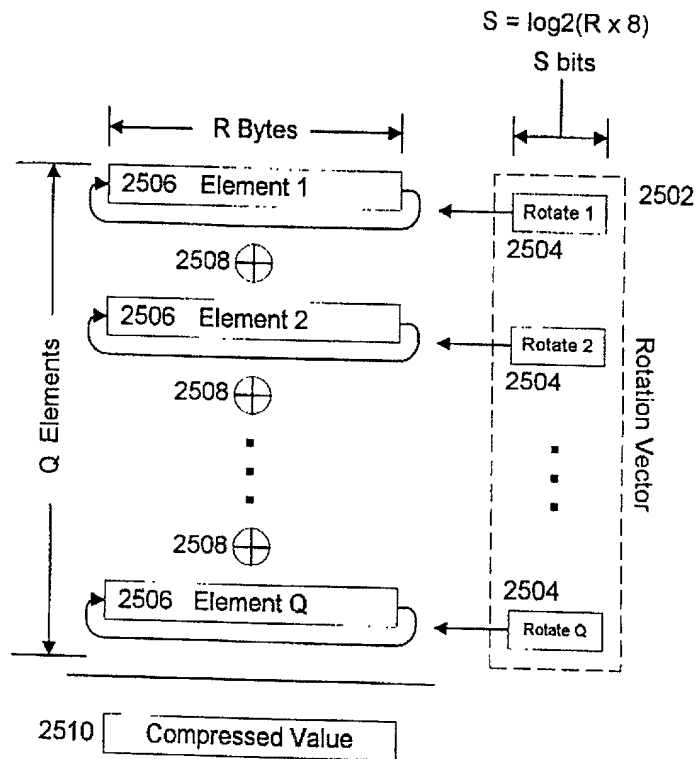


Fig. 26

Compressing a 64 Kilobyte Message

2602

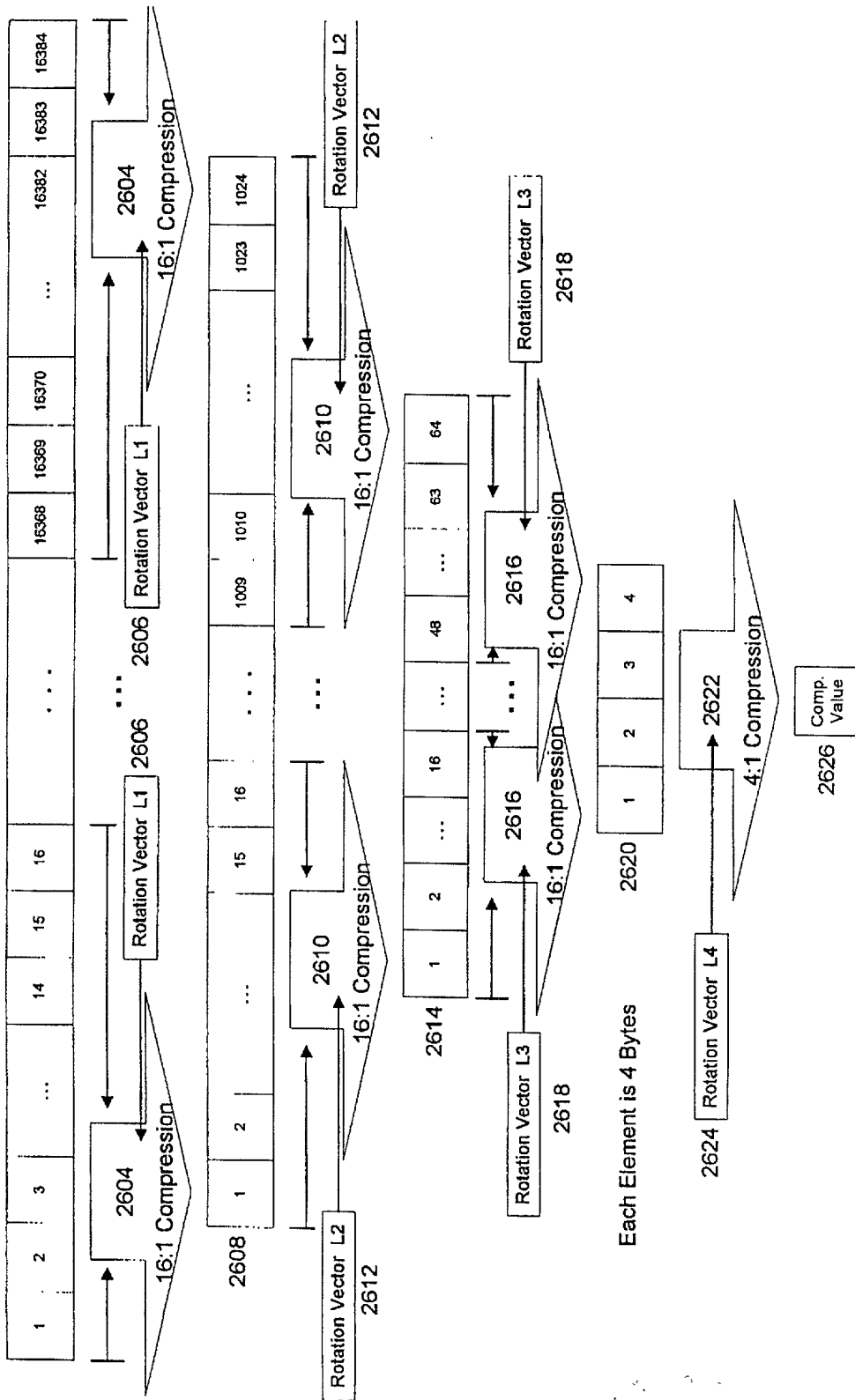


Fig. 27

Compressing a 64 Byte Message

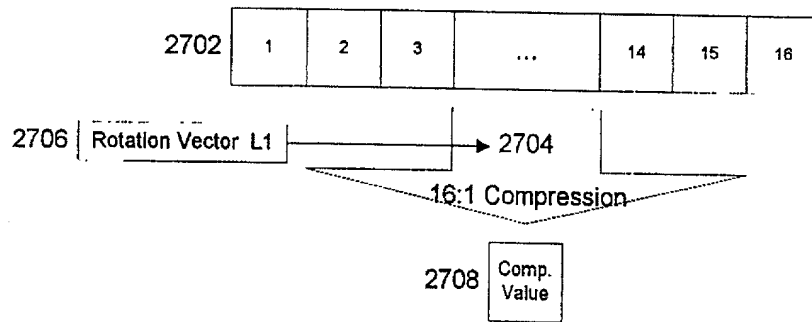


Fig. 28

Compressing a 1518 Byte Message

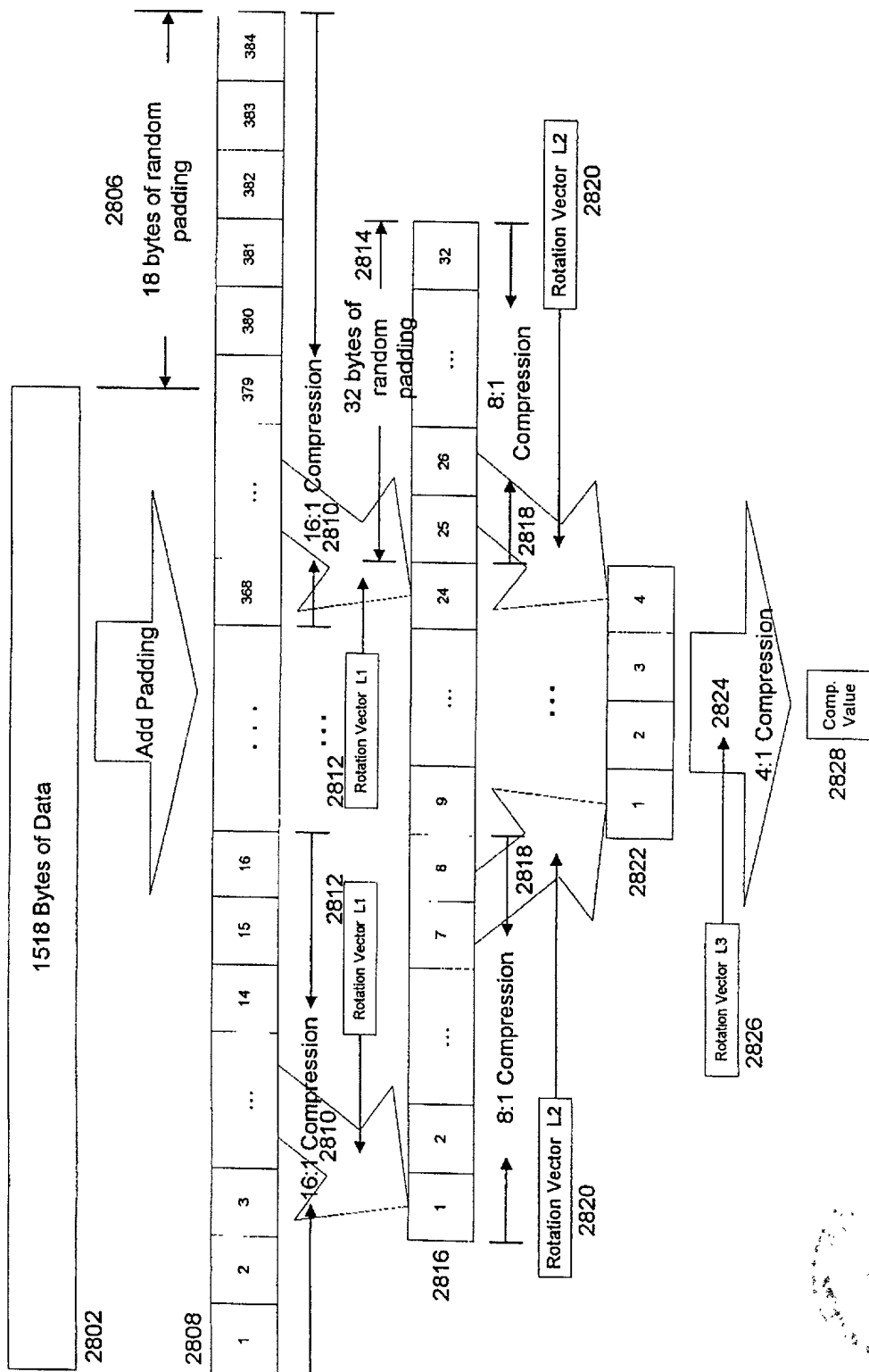


Fig. 29

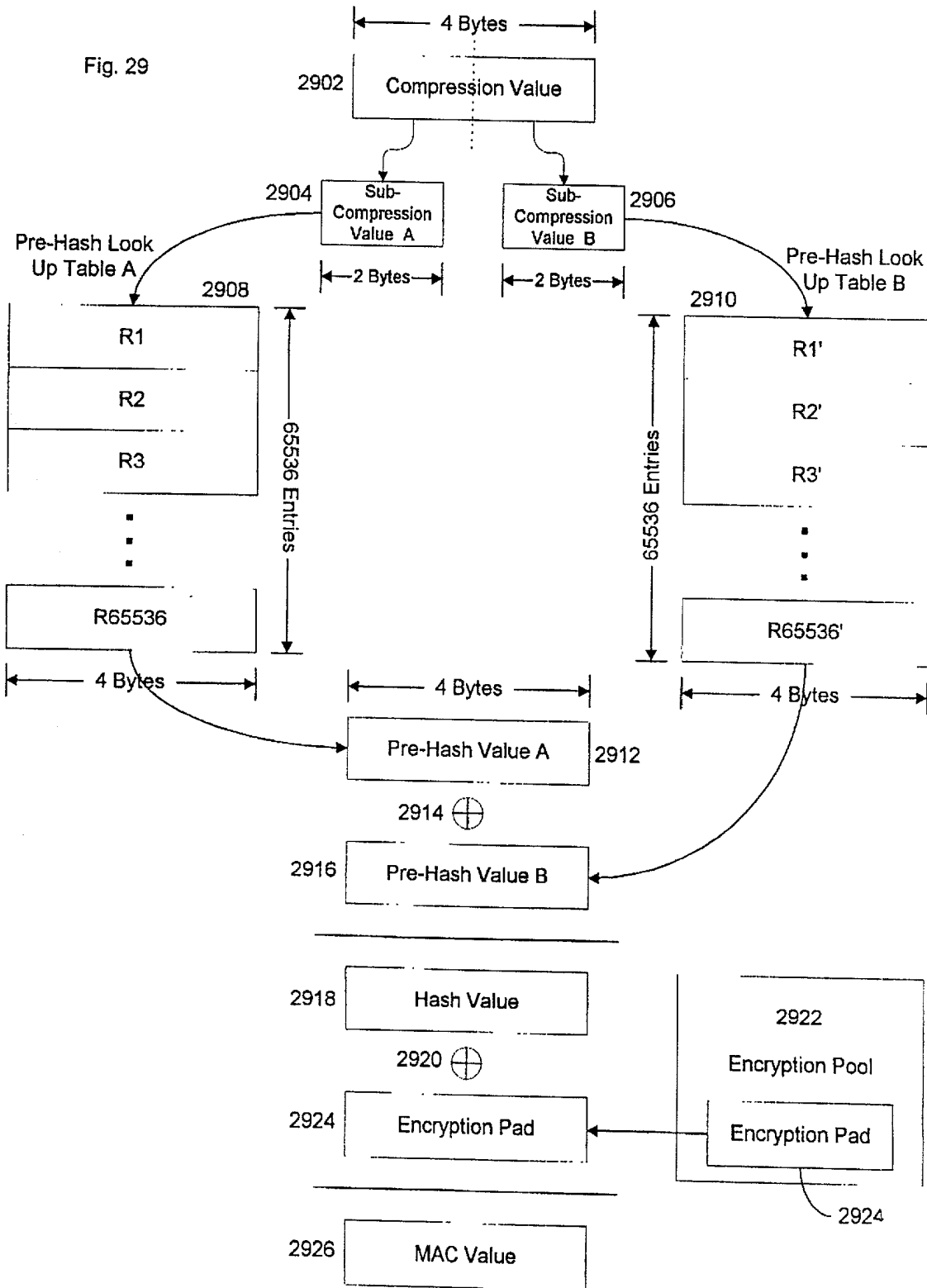


Fig. 30

Shuffling a Pre-Hash Look Up Table (256 KB)

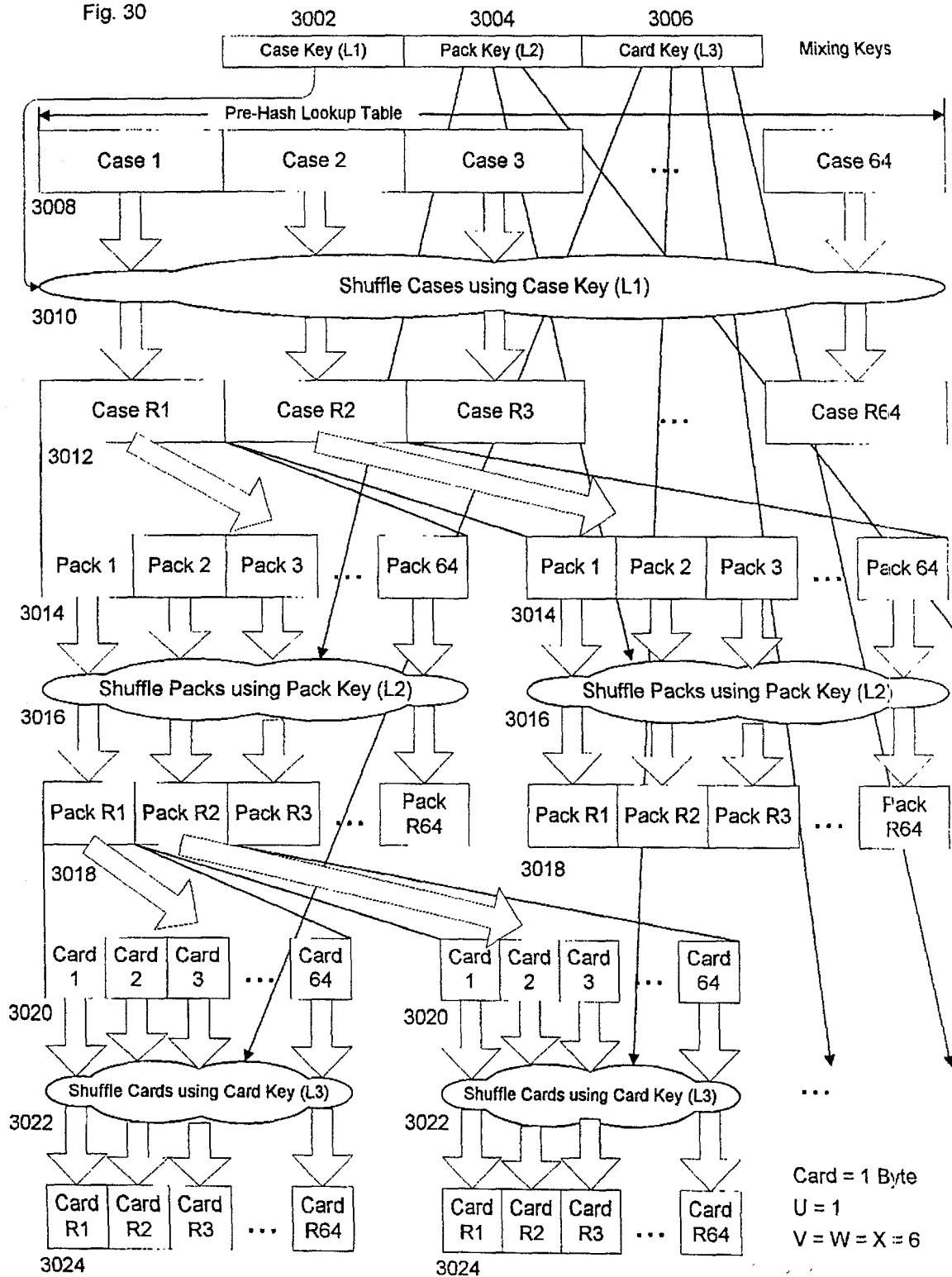


Fig. 31

Shuffling an Encryption Pool (512 Bytes)

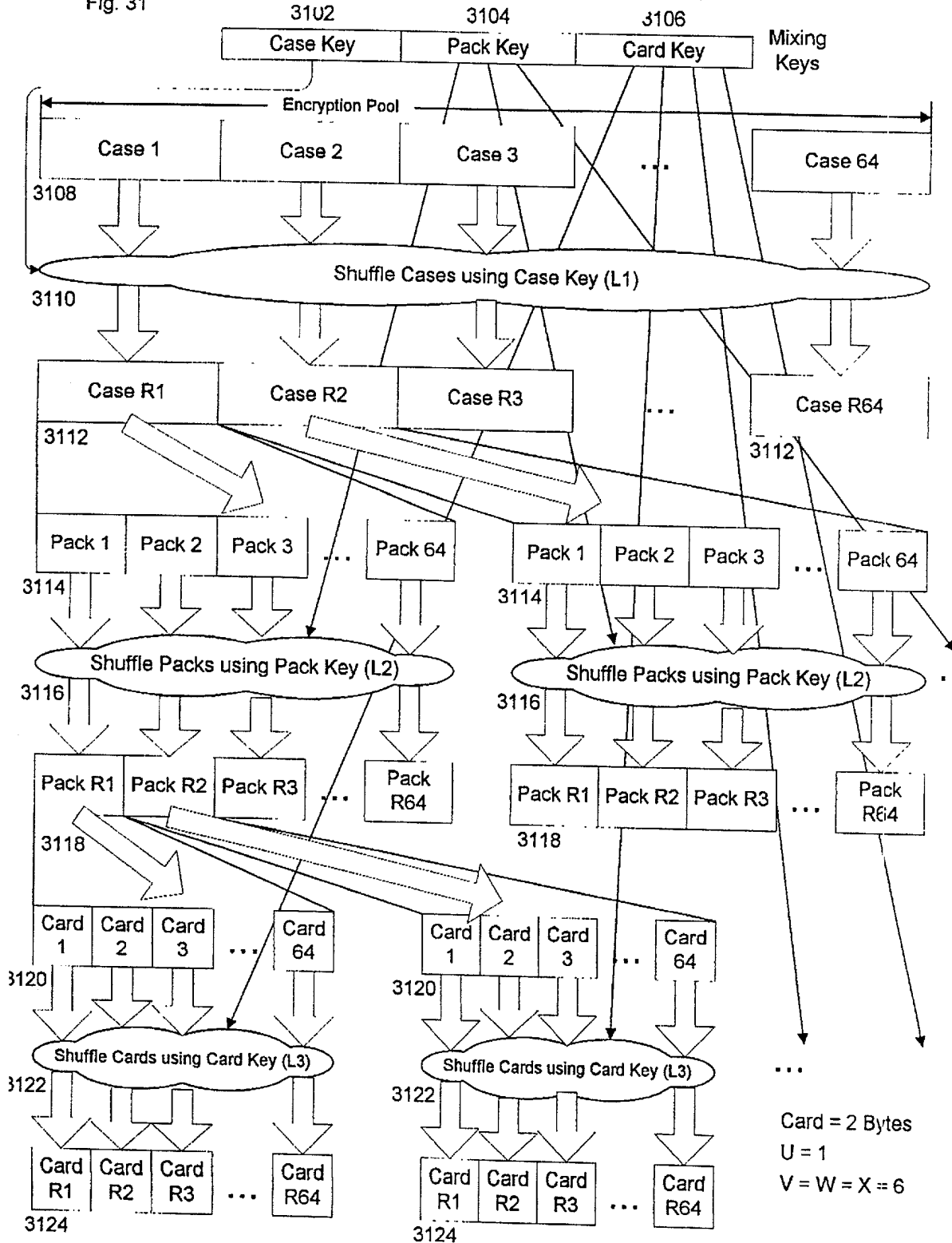


Fig. 32

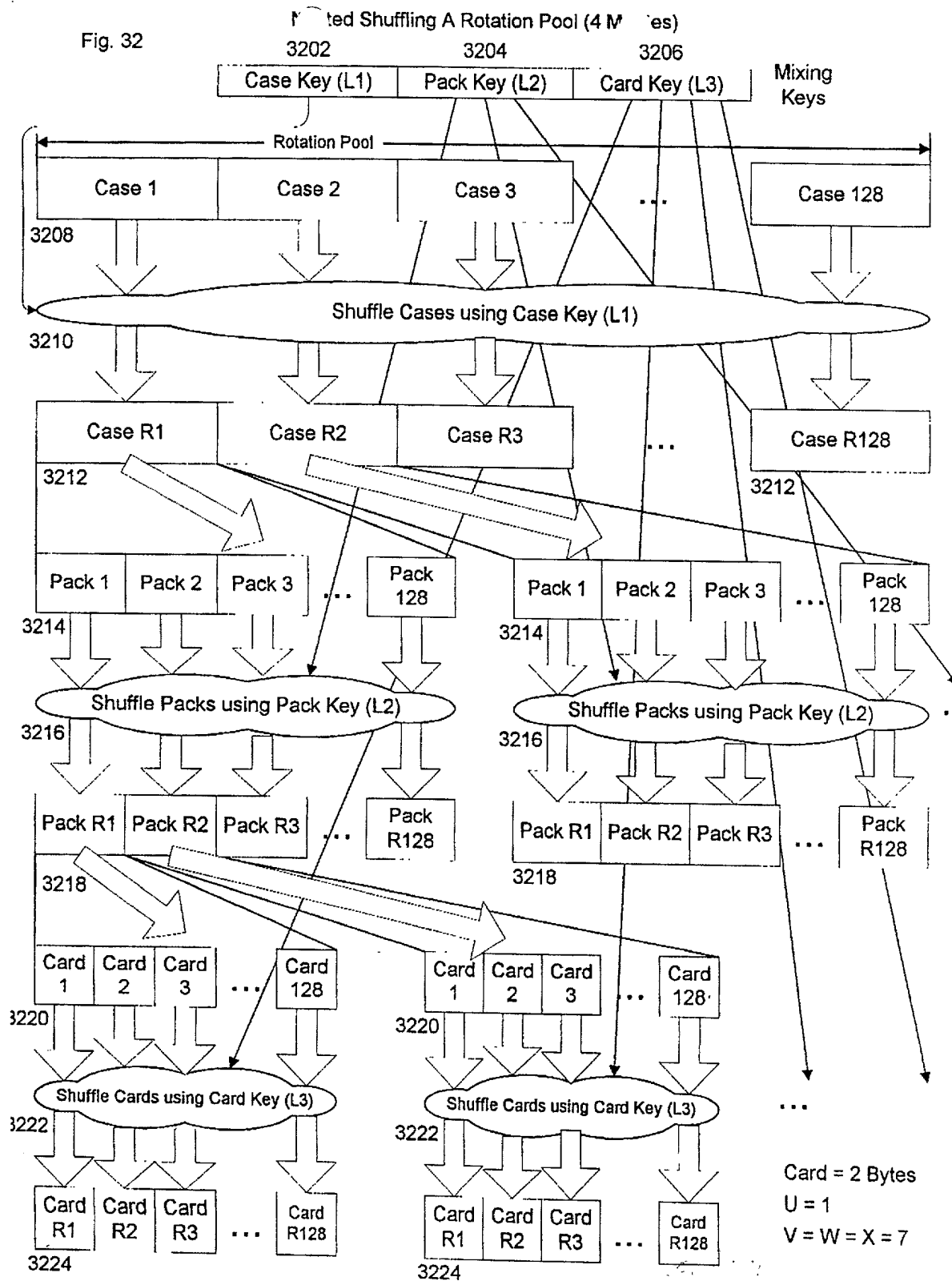


Fig. 33

Shuffling A Padding Pool (256KP)

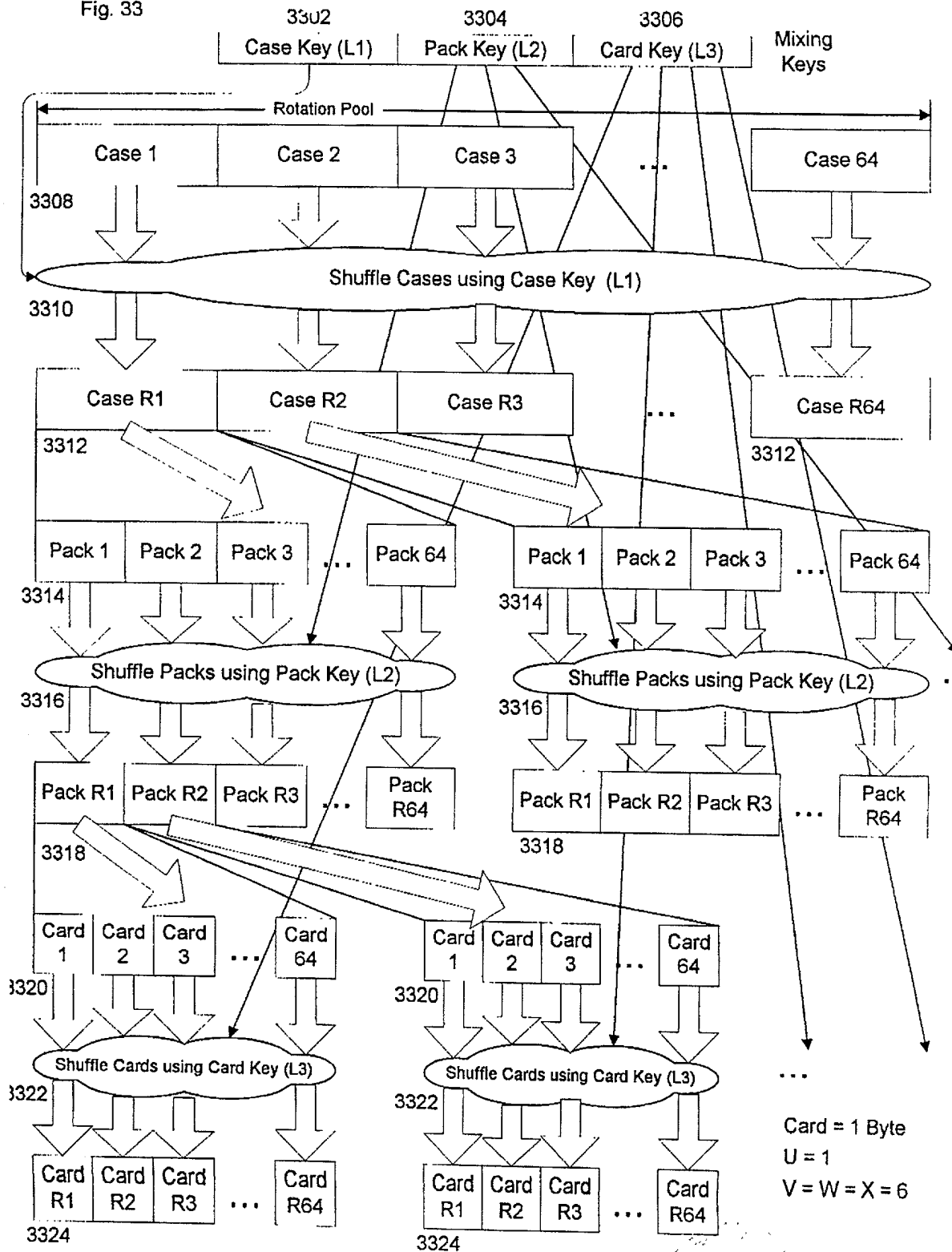
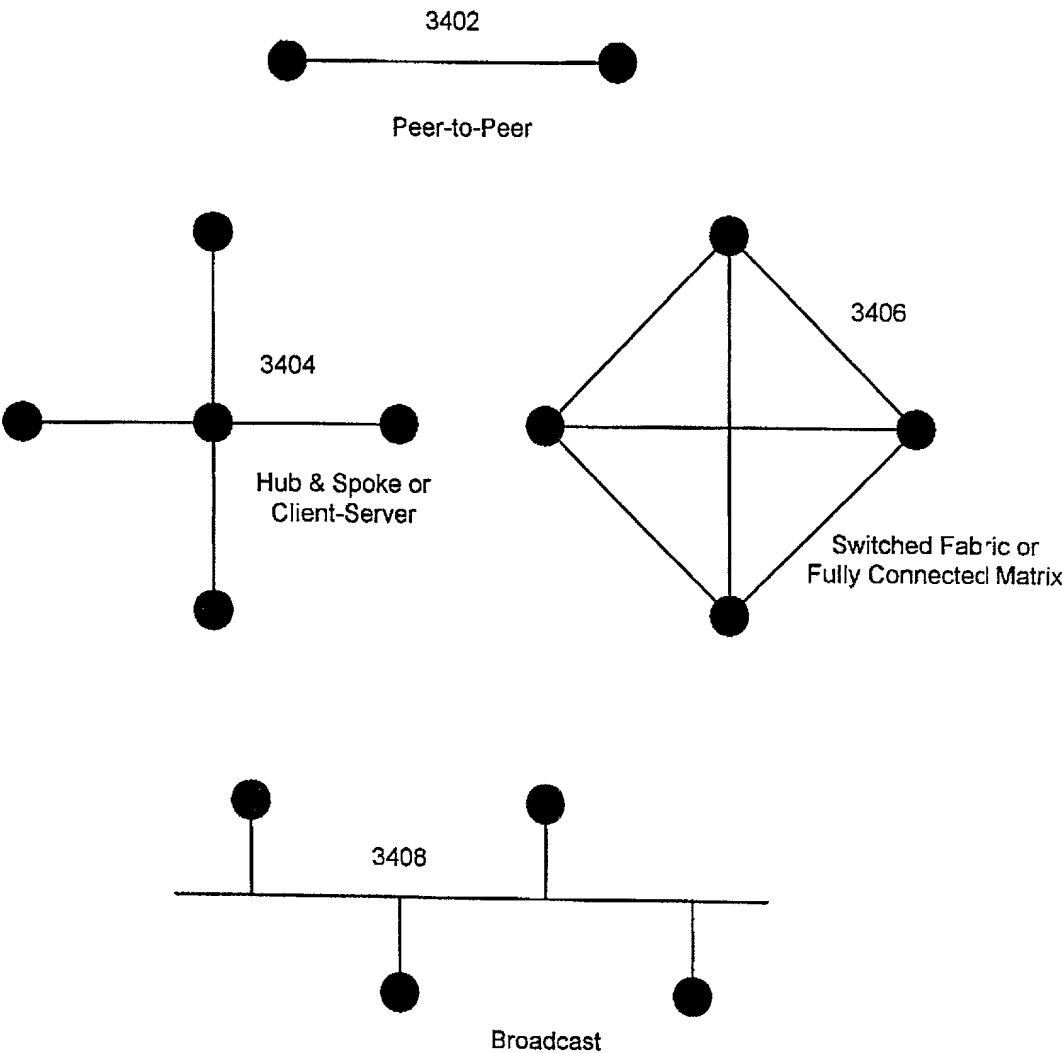


Fig. 34



2025 RELEASE UNDER E.O. 14176